School of Engineering and Applied Science (SEAS), Ahmedabad University

B.Tech(ICT) Semester V: Wireless Communication (CSE 311)

- Group No : PLS S14

1 Performance Analysis of Base Article

- List of symbols and their description

Symbol	Description
$\alpha - \eta - \kappa - \mu$	Channel Capacity of a wireless vehicular communication is analyzed over this fading channel.
P	Primary static user
E	Passive eavesdropper
S	Legitimate transmitter
R	Legitimate receiver
R"	Relay node
x	Transmitted signal symbol
	Chanel coefficient between legitimate transmitter and relay node1
	Chanel coefficient between relay node1 and legitimate receiver
n_R	Complex hardware additive white gaussian noise at legitimate receiver
n_{R00}	Complex hardware additive white Gaussian noise at relay node
$f_R(r)$	PDF of the channel model of $\alpha - \eta - \kappa - \mu$
α	Non-linearity parameter of the medium
κ	Ratio of total power of dominant components to the scattered total power
	Channel gain
	The distribution of the distance d

Continued on next page....

Table 1 – Continued from previous page....

Symbol	Description
$F_Z(z)$	CDF of the channel model.

	Channel gain
	The distribution of the distance d
	CDF of the channel model.
γ	Instantaneous SNR
P_{out}	Threshold SNR
	Outage probability that the received instantaneous SNR falls below a threshold γ_{th}
$P_\gamma(\gamma)$	PDF of SNR γ
γ_E	Received SNR at eavesdropper
	Received SNR at legitimate receiver
	The instantaneous secrecy capacity
	The transmitter power for cognitive network
	Interference power
	Secrecy outage probability

- SYSTEM MODEL

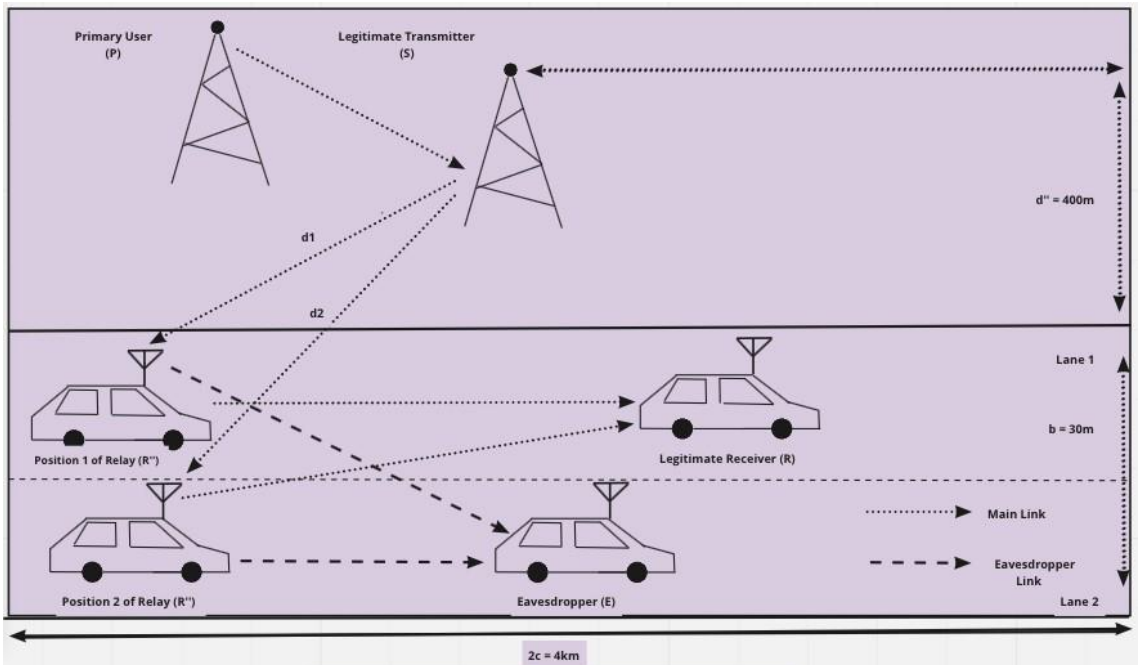

Figure 1 : Highway vehicular network model

In this section, we have considered a cognitive radio based network consisting of one legitimate transmitter and one legitimate receiver in the presence of one eavesdropper. Each user is equipped with a single antenna.

→ **Network Model :**

As we can see in the above figure, this is a two-lane highway cognitive vehicular network. S denotes the legitimate static transmitter. R", R, and E represent the position of relay, legitimate receiver and eavesdropper respectively. The road length is 2c and width is b.

The network model illustrates the location of relay under two scenarios.

Case 1 : Relay is nearer to legitimate transmitter **Case 2 :** Relay is at far distance from legitimate transmitter.

→ **Channel Model :**

The initial positions of relay vehicle (R") from legitimate transmitter is shown in system model. Here, vehicle (E) performs the role of a passive eavesdropper. The relay vehicle is allowed to receive information after the resource allocation has been provided in a cognitive radio-based network. The CSI is considered to be perfect. The channel model of $\alpha - \eta - \kappa - \mu$ is considered as follows:

$$f_R(r) = \frac{\alpha r^{\alpha\mu-1} \sum_{k=0}^{\infty} \frac{k! c_k L_k^{\mu-1}(2r^{\alpha})}{(\mu)_k}}{2^{\mu}\Gamma(\mu)\exp(\frac{r^{\alpha}}{2})} \quad (1)$$

The description of each symbol is shown in Table-1.

→ **Signal Model:** The signal model at relay nodes and legitimate receiver in the presence of one eavesdropper is defined in this section. At first, the signal is received by relay nodes (R") which is then transmitted and received by legitimate receiver (R).

Let's first define the signal received by relay node R":

$$y(t) = h_{SR"}(t)x(t) + n_{R"}(t) \quad (2)$$

The channel gain h is given by:

$$h_{SR"}(t) = \frac{g_x}{\sqrt{1 + d_x^{\zeta}(t)}} \quad (3)$$

The description of each symbol is shown in Table-1.

Moreover, the received signal after amplifying and forwarding at the legitimate transmitter is given as:

$$y^0(t) = h_{R"R}(t)y(t) + n_R(t) = h_{R"R}(t)(h_{SR"}(t)x(t) + n_{R"}(t)) + n_R(t) \quad (4)$$

• STATISTICAL KNOWLEDGE OF RECEIVED SIGNAL TO NOISE RATIO UNDER MOBILITY

To evaluate the received SNR under the vehicle mobility can be derived for $\alpha - \eta - \kappa - \mu$ fading chanel by PDF of SNR.

So, first we have to calculate CDF of the channel model.

For CDF the general formula is given as:

$$F_Z(z)_{case1} = \int_0^{\infty} \int^{yz} f \quad f \quad dxdy_{-\infty} \quad {}_x(x) \; {}_y(y) \tag{5}$$

Here, we have a two different cases.

Case1 is relay is nearer to legitimate transmitter(Position 1) and case2 is Relay is at far distance from legitimate transmitter(Position 2).

In equation (5) for each case, $f_X(x)$ and $f_Y(y)$ is replaced by the independent distribution of fading channel and distance respectively.

→ Case1 :

The PDF of distance between SU and PU is defined as Eq.(6). By substituting Eq.(6) and Eq.(1) in the Eq.(5), the CDF is obtained for the case1 is in Eq.(7).

$$f_y(y)^{case1} = \frac{d}{4\mathrm{ab}} \left(2\sin^{-1} \left(\frac{2\left(y^2 - (b-h)^2\right)}{y^2} \right) + \pi - 1 \qquad ! \right. \tag{6}$$

$$F_z(z)^{case1} = \frac{\alpha \mathrm{r}^{\alpha\mu-1} \int_0^{\infty} \int_{-\infty}^{yz} \frac{d}{4\mathrm{ab}} \left(2\sin^{-1} \left(\frac{2\left(y^2-(b-h)^2\right)}{y^2} \right) + \pi - 1 \right) \sum_{k=0}^{\infty} \frac{2k! c_k r^{\alpha} L_k^{\mu-1}}{\mu_k} drdy}{\Gamma(\mu) * e^{\frac{r^{\alpha}}{2}} * 2^{\mu}} \tag{7}$$

Further to evaluate the PDF of SNR for case1, Eq.(7) is differentiated. So, the PDF of SNR for case 1 is in Eq.(8).

$$p_\gamma(\gamma)_{case1} = \frac{\left(\frac{\gamma\mu}{\overline{\gamma}}\right)^{d(\mu-1)} exp\left(\frac{-\gamma}{\overline{\gamma}\times(1-(\alpha))}\right) \times F_1\left(k, 1/2ab; \frac{\mu \times det(\alpha) d}{1-det(\alpha+2d)}\right)}{(1-det(\mu))^d} \tag{8}$$

→ Case2 :

The PDF of distance for this case d is given as Eq.(9). By substituting Eq.(9) and Eq.(1) in the Eq.(5), the CDF is obtained for the case2 is in Eq.(10).

!# $$f_y(y)^{case2} = \frac{d}{2ab}\left[\arcsin\left(\frac{2\left(d^2-d_p^2\right)}{d^2}-1\right)-\arcsin\left(\frac{2\left(d^2-h^2\right)}{d^2}-1\right.\right. \quad (9)$$

$$F_z(z)^{case1} = \frac{\alpha r^{\alpha\mu-1}\int_0^{\infty}\int_{-\infty}^{yz}\frac{d}{2ab}\left(\sin^{-1}\left(\frac{2\left(d^2-d_p^2\right)}{d^2}-1\right)-\sin^{-1}\left(\frac{2\left(d^2-h^2\right)}{d^2}-1\right)\right)\sum_{k=0}^{\infty}\frac{2k!c_k r^{\alpha}L_k^{\mu-1}}{\mu_k}drdy}{\Gamma(\mu)*e^{\frac{r\alpha}{2}}*2^{\mu}} \quad (10)$$

Further to evaluate the PDF of SNR for case2, Eq.(10) is differentiated. So, the PDF of SNR for case 1 is in Eq.(11).

$$p_\gamma(\gamma)_{case2} = \frac{\left(\frac{\gamma\mu}{\overline{\gamma}}\right)^{d(\mu-1)} exp\left(\frac{-\gamma}{\overline{\gamma}\times(1-(\alpha))}\right)\times\beta(i,j,k,l)}{(1-det(\mu))^d} \quad (11)$$

- ANALYSIS OF THE OUTAGE PROBABILITY.

Outage probability means that the received instantaneous SNR γ falls below a some threshold γ_{th}.
To evaluate an outage probability the generak formulas is given in Eq.(12) and Eq.(13).

$$P_{\text{out}} = \Pr(0 \le \gamma \le \gamma_{th}) \quad (12)$$

$$P_{\text{out}} = \int_0^{\gamma_{th}} f_\gamma(\gamma)dz \quad (13)$$

Here we have PDF of SNR for two different cases so the outage probability is different for two cases.

$$P_{outcase1} = \int_0^{\gamma_{th}} p_\gamma(\gamma)_{case1}d\gamma \quad (14)$$

$$P_{out}^{case2} = \int_0^{\gamma_{th}} p_\gamma(\gamma)_{case2}d\gamma \quad (15)$$

Further to evaluate the outage probability for case1, Eq.(8) substituting in the Eq.(14), outage probability for case1 is obtained in Eq.(16).

$$P_{out}^{case1} = 1 - e^{\frac{ab}{z_{th}}}\sum_{z=1}^{T_k}\sum_{n=0}^{\alpha}\Gamma(e^{z-1}+z) + (\frac{\alpha^3}{2e^{-d}}+\eta^2)C_k + D_k \quad (16)$$

Same as to evaluate the outage probability for case2, Eq.(11) substituting in the Eq.(15), outage probability for case2 is obtained in Eq.(17).

$$P_{out}^{case2} = 1 - e^{\frac{ab}{z_{th}}}\sum_{z=1}^{T_k}\sum_{n=0}^{\alpha}\Gamma(e^{\mu-1}+z^n) + (\frac{\psi^3}{2e^{-d}}+\eta^2)F_k + E_k \quad (17)$$

- ANALYSIS OF THE SECRECY OUTAGE PROBABILITY.

To evaluate the SOP at the passive eavesdropper side for two different cases first we have to obtain the secrecy capacity.

The instantaneous secrecy capacity is :

$$C_s(\gamma_E,\gamma_R) = max\{ln(1+\gamma_E) - ln(1+\gamma_R),0\} \tag{18}$$

Where γ_E is the received SNR at eavesdropper and γ_R is the received SNR at legitimate receiver.

R_s is a constant code rate.

$$\Pr\{C_s(\gamma_R,\gamma_E) \leq R_s\} \tag{19}$$

So, the SOP can be evaluate as:

$$P_{\text{sop}} = \underbrace{\Pr\left\{C_s\left(\gamma_R,\gamma_E\right) \leq R_s, P_s = P_{\max}\right\}}_{I_1} + \underbrace{\Pr\left\{C_s\left(\gamma_R,\gamma_E\right) \leq R_s, P_s = \frac{I_p}{X}\right\}}_{I_2} \tag{20}$$

Where P_s is the transmitter power and it can be expressed as:

$$P_s = \min\left(P_{\max}, \frac{I_p}{X}\right) \tag{21}$$

Where X is a channel gain between primary transmitter and legitimate transmitter, I_p is the interference power, P_{max} is the maximum transmitted power.

In Eq.(20) formula is used to derive the SOP for both the cases, the integral is divided into several sub integral under certain equality such as when $P_s = P_{max}$, the integral I1 is given as :

$$\begin{aligned} I_1 &= \Pr\left\{C_s\left(\gamma_R,\gamma_E\right) \leq R_s, P_s = P_{\max}\right\} \\ &= \Pr\left\{Z_R \leq \theta Z_E + \frac{\theta-1}{\alpha}\right\} \Pr\left\{x \leq \frac{I_P}{P_{\max}}\right\} \end{aligned} \tag{22}$$

And the integral I_2 is given as :

$$I_2 = \int_{I_p/P_{Max}}^{\infty} H(x) f_X(x) dx \tag{23}$$

Where, H(x) is the PDF of fading channel as per Eq.(1) and $f_x(x)$ can be replaced as PDF of received SNR for case 1 and case 2.

Hence the final expression of the SOP is the summation of the derivation I1 and I2 as per Eq.(24).

$$P_{SOP}^{Case1} = \frac{\alpha_E 2^{-(\mu_E+\mu_R+2)} \overline{\gamma_R}^{\frac{-\alpha_B\mu_R}{2}}}{\Gamma(\mu_E)\Gamma(\mu_R)\overline{\gamma_E}^{\frac{\alpha_E A_R}{2}}} \sum_{n=0}^{\infty} \frac{n! c_{n,E}}{(\mu_E)_n} \sum_{s=0}^{n} T_1 \tag{24}$$

$$P_{SOP}^{Case2} = A_k B_k \sum_{n=1}^{\infty} \lambda_k^n z^{\mu} \frac{e^{z/cb}(1/ab)}{d^2} + C_k D_k \sum_{n=1}^{\infty} \lambda_k^n \frac{e^{z/cb}(1/cb)}{d^2} + \eta\sqrt{\alpha} \tag{25}$$

2 Numerical Results

2.1 Simulation Framework

In order to verify the accuracy of the above derived expressions of outage probability and secrecy outage probability we need to have some controlling parameters to be in simulation.

- The values of R_s(code rate) and P_{max}(maximum power transmitted) are to be considered as 0.1bits/Hz and 1 W respectively.

- The outage probability at the relay nodes depends on the vehicle velocity and also on the SNR at that point.

- Since the outage is stated as the probability that SNR γ is below the γth threshold. Thus γth is a major controlling parameter for outage probability.

- For all cases we had considered a fix velocity for obtaining the behaviour of the outage probability.

- Instantaneous secrecy capacity C_s and the transmitter power are the major parameters for the Secrecy Outage Probability.

- The SNR γ values at the eavesdropper side is to be considered as very high in order to evaluate the asymptotic performance of the secrecy outage probability.

2.2 Reproduced Figures

- Reproduced Figure-1

  In two lane highway scenario, outage probability shows that the conditions for outage is dependent on vehicular velocity and the SNR at relay node. Hence, we consider fixed velocity to obtain behavior of the outage probability. The analysis is carried out for the eavesdropper side. Hence, we focus on the velocity of the eavesdropper rather than the legitimate receiver because the aim is to get over the capability of the eavesdropping. In cognitive radio systems, under certain fix interference power and velocity, the secrecy outage is dependent on the fading parameter between the relay node and legitimate receiver. These results are obtained for best values of α, κ, and μ (i.e. α = 1, κ = 1, and μ = 1).

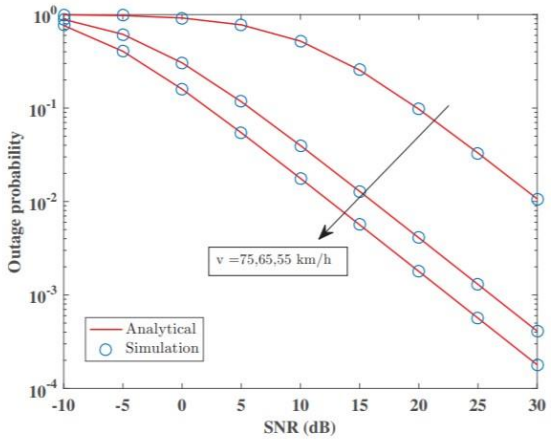

Figure 1B

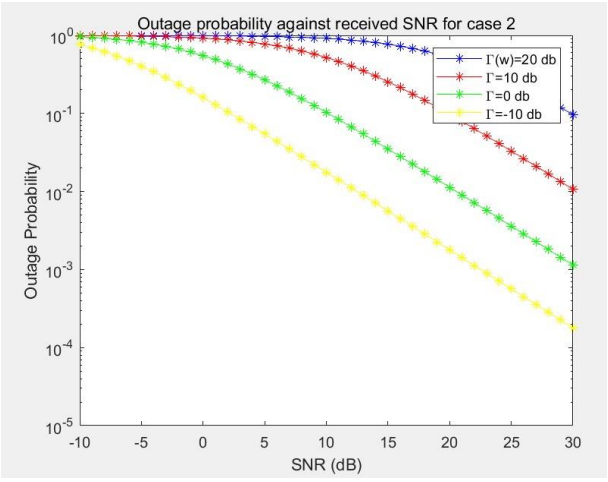

Figure 1R

The outage probability performance when relay node is at far distance form legitimate transmitter is shown in figure 1R. As stated in above figure, the fixed velocity of eavesdropper is 55, 65, and 75 respectively. Under the specific fading parameter(i.e. α = 1, κ = 1, and μ = 1) and fix velocity, the OP performance is degraded with the increased velocity but the variation in degradation is high. Hence, when the relay node is at far distance from the legitimate transmitter, SNR requirement for secure transmission is high for higher velocity.

- Reproduced Figure-2

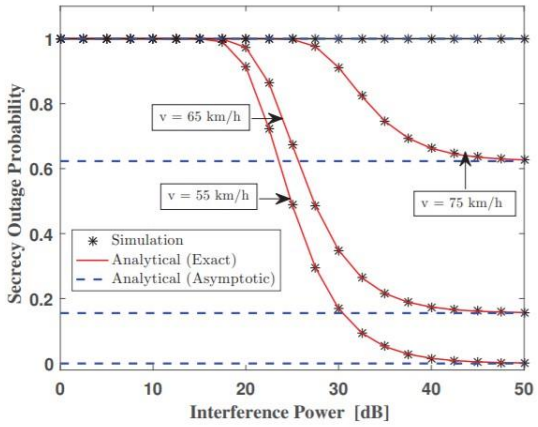

Figure 2B(Case1)

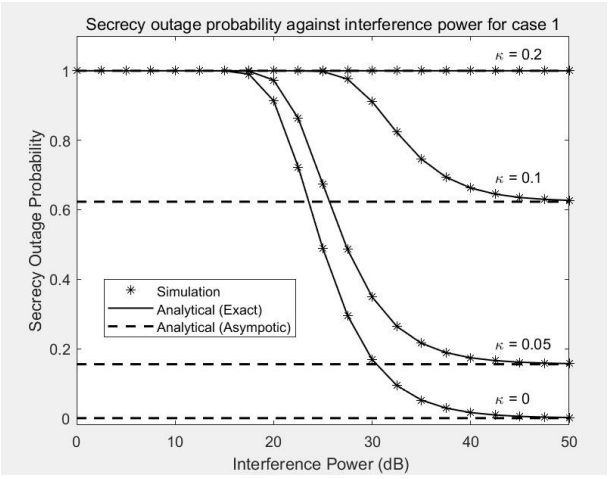

Figure 2R(Case1)

The secrecy outage probability performance when relay node is nearer to legitimate transmitter is shown in figure 2R(case1). As stated in above figure, the fixed velocity of eavesdropper is 55, 65, and 75 respectively. Under the specific fading parameter(i.e. α = 1, κ = 1, and μ = 1) and fix velocity, the SOP performance is degraded with the increased velocity but the variation in degradation is low compared to case2. Hence, when the relay

node is nearer to the legitimate transmitter, SNR or secrecy rate requirement for secure transmission is higher for higher velocity.

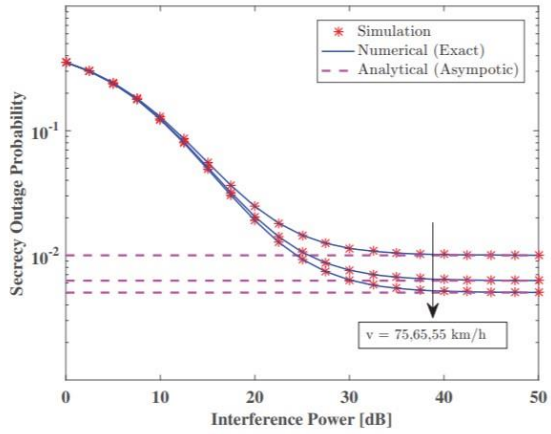

Figure 2B(Case2)

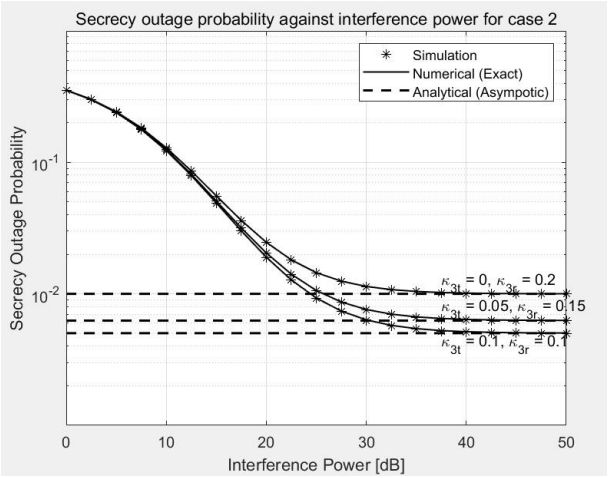

Figure 2R(Case2)

The secrecy outage probability performance when relay node is at far distance form legitimate transmitter is shown in figure 2R(case2) is stated in above figure, the fixed velocity of eavesdropper is 55, 65, and 75 respectively. Under the specific fading parameter(i.e. α = 1, κ = 0, and μ = 1) and fix velocity, the SOP performance is degraded with the increased velocity but the variation in degradation is high. Hence, when the relay node is at far distance from the legitimate transmitter, SNR or secrecy rate requirement for secure transmission is lower for higher velocity.

References

[1] S. Kavaiya, D. K. Patel, Y. L. Guan, S. Sun, Y. C. Chang, and J. M.-Y. Lim, "On Physical Layer Security over $\alpha-\eta-\kappa-\mu$ Fading for Relay based Vehicular Networks," *2020 International Conference on Signal Processing and Communications (SPCOM)*, 07 2020.